

**REMARKS**

Claims 2–25 were previously pending in this application. Applicant has amended claims 2, 5, 8, and 10. As a result, claims 2–25 are pending with claims 2, 8, 13, 18, 22, 23, 24, and 25 being independent claims. No new matter has been added.

Please amend the Attorney Docket Number from 212515 to MS# 177765.01.

Rejection of Claims 2–12, 22, and 23

Claims 2, 8, 9, 22, and 23 stand rejected under 35 U.S.C. § 103(a) as being obvious over U.S. Patent No. 6,092,201 to Turnbull [hereinafter Turnbull] in view of U.S. Patent No. 6,748,530 to Aoki [hereinafter Aoki]. Applicant respectfully responds to the rejection as follows:

Claim 2

Applicant agrees with the Examiner's statement that "Turnbull does not teach signing with a group public/private key pair." However, even if Aoki showed using a group private key to sign a shared list of Turnbull, as suggested by the Examiner, such a combination does not teach using the certificate to *invite* a user to a peer-to-peer group, much less allow the user to *connect to* the peer-to-peer group through a second user. Specifically, independent claim 2 recites, *inter alia*, sending the group certificate to the peer to *invite* the peer to join the group, the group membership certificate allowing the peer to join the group through a second member other than the first member. More particularly, the shared list of Turnbull and the group certificate of Aoki are used to access the individual public keys of listed users, and there is no teaching or suggestion in either Turnbull or Aoki of the certificate being used by an individual member to *join* a secure peer-to-peer group after *receiving an invitation*.

Type of Response: Amendment after FINAL

Application Number: 09/955,924

Attorney Docket Number: 177765.01

Filing Date: 09/19/2001

In the Final Office Action, the Examiner suggests that Turnbull teaches the features of claim 2, by suggesting “the invitation of the user 2 by the user 1 to join the group is interpreted based on the situation that the originating user 1 would also be required to be authenticated by the invited user 2 via validating the originating user’s signature.” (*Office Action*, page 3). However, in Turnbull, the listed member validates the originating user’s signature *only if the member desires to access* and use the list. As such, list member validation of the originating user’s signature cannot be considered an invitation since it is initiated by and actual member of the list (not an invitee who is not currently a member) and is not initiated by the originating user.

Claim 2 also recites, *inter alia*, a method of inviting and joining a *peer* to a *secure peer-to-peer group* and sending the group certificate to the peer to invite the peer to join the group. The primary reference of Turnbull does not teach or suggest inviting and joining a *peer* to a *secure peer-to-peer group*, which is defined in Applicant’s specification as a group formed within a peer-to-peer network. (*See, e.g.,* paras. [0002], [0008], [0009], [0034]). Rather, Turnbull suggests creating a shared list of certificates to extend secure communications between users, which are not described as peers of a peer-to-peer network.

In the Advisory Action, the Examiner states that to ‘invite’ means to ‘request formally’. The Examiner then implies an invitation when a member of the list of Turnbull uses and verifies the signature of the list. Specifically, the Examiner implies that the mutual authentications (e.g., when the creating user creates the list and when the member user uses the list) is a ‘formal request’ or ‘invitation’. Applicant is unable to see how *authentication* of the member when the list is generated and *authentication* of the public key of the creating user by the member user to verify the list forms a ‘formal request’ or invitation. Specifically, the two authentications of signatures are independent in time and function, and thus do not together form a formal request or

Type of Response: Amendment after FINAL

Application Number: 09/955,924

Attorney Docket Number: 177765.01

Filing Date: 09/19/2001

invitation. Thus, Turnbull and Aoki, either alone or in combination, do not teach or suggest a method of inviting and joining a peer to a secure peer-to-peer group as recited in claim 2.

Moreover, even if such an independent authentication of the list in Turnbull was an invitation, the authentications do not teach or suggest the features of claim 2 as amended including receiving, at a second member of the group different from the first member, a *connect message* from the peer containing the group membership certificate, the connect message *requesting connection* to the secure peer-to-peer group; and the second member, authenticating the group membership certificate before allowing the peer to connect to the secure peer-to-peer group.

In the Advisory Action, the Examiner suggests that Turnbull teaches the features of claim 2 (the certificate allowing a peer to join the group through a second member other than the first member), by suggesting that a 'shared list authorization field' indicates whether a user may modify a list that was created by itself or by another user and verifying whether a user is authorized to modify by checking its signature verification. If the Examiner is suggesting that a first user may create the shared list, a second user may modify the shared list, and the modification by the second user may add the member user (e.g., peer) to the 'group' of the shared list, this suggested interpretation does not teach or suggest the features of claim 2. Specifically, if the second member modifies a shared list created by a first member to include a peer, then such a modification does not teach or suggest forming the certificate with the peer's secure communication information by the first member as recited in claim 2. If the Examiner is suggesting that a first user may create the list, a second user may modify the list, and to verify whether the second user is authorized, its signature is checked in the shared list authorization field, then this suggestion also does not teach or suggest the features of claim 2. Specifically, the Examiner's suggestion does not introduce a

Type of Response: Amendment after FINAL

Application Number: 09/955,924

Attorney Docket Number: 177765.01

Filing Date: 09/19/2001

second *member* of the group different from the first *member*. More particularly, the only actors in the Examiner's suggestion is the originating user (suggested first member by the Examiner) and the modifying user (the peer as suggested by the Examiner). Thus, the suggested interpretation of Turnbull of a modifying user does not teach or suggest a certificate allowing a peer to join the group through a second member other than the first member as recited in claim 2.

Accordingly, claim 2 patentably distinguishes over Turnbull in view of Aoki such that the rejection under § 103 should be withdrawn. Claims 3–7 depend from independent claim 2, and are patentable for at least the foregoing reasons.

Claim 22

Claim 22 recites a computer-readable medium having computer executable instructions for performing the steps of claim 2. Accordingly, claim 22 is patentable for at least the foregoing reasons.

Claim 8

Claim 8 recites, *inter alia*, forming by the first member a first group membership certificate containing the peer's public key ( $P_{U1}$ ) and a second group certificate signed with the group private key ( $K_G$ ), the first group membership certificate being signed with a private key of the first member ( $K_{U2}$ ). As noted above with respect to claim 2, Applicant agrees with the Examiner's statement that "Turnbull does not teach signing with a group public/private key pair." However, even if Aoki taught signing a certificate with a group private key, such a combination does not teach or suggest the recited features of claim 8.

In the Advisory Action, the Examiner states that Turnbull teaches a first certificate containing the peer's public key and Aoki teaches a second certificate sign with the group private key. It appears that the Examiner is combining the teachings of Turnbull and Aoki in a completely different manner in the rejection of claim 8 as

Type of Response: Amendment after FINAL

Application Number: 09/955,924

Attorney Docket Number: 177765.01

Filing Date: 09/19/2001

compared to the combination of the same references in the rejection of claim 2 above. Specifically, the Examiner in rejecting claim 2, equates the shared list of Turnbull with the certificate of Aoki to achieve a shared list of Turnbull signed by a group private key of Aoki. In contrast, in rejecting claim 8, the Examiner states that in a combination of the same references, the shared list of Turnbull and the certificate of Aoki are no longer equivalent, but rather independent and stand apart. Thus, it appears that the Examiner is using inappropriate hindsight to reject Applicant's claims.

Despite this difference in results of a combination of the same references, the Examiner does not provide any further motivation to combine Turnbull and Aoki in this 'new' way. More particularly, the Examiner has provided no motivation to combine the cited references which suggests a desire or need to keep separate the shared list of Turnbull and the certificate of Aoki. More particularly, if the cited combination of Turnbull and Aoki teaches that the group private key of Aoki may be used both *in place of* the authorized person's private key (as suggested in rejecting claim 2), then the same cited combination of Turnbull and Aoki cannot teach or suggest that the group private key of Aoki be used *in addition to* the authorized person's private key (as suggested in rejecting claim 8). Thus, the combination of Turnbull and Aoki does not teach or suggest the features of claim 8.

Even if Aoki and Turnbull showed using a group private key to sign a certificate and a private key of an authorized person to sign a shared list, the combination does not teach or suggest the features of claim 8 of sending the first and second group certificates from the first member to the peer to *invite* the peer to join the group, and receiving, at a second member different from the first member, *a connect message* from the peer containing the first group membership certificate as recited the amended claim 8. As noted above with respect to claim 2, the shared list of Turnbull and the certificate of Aoki are not used to *enter* a group, but rather, to save encryption schemes for a list

Type of Response: Amendment after FINAL  
Application Number: 09/955,924  
Attorney Docket Number: 177765.01  
Filing Date: 09/19/2001

of users to be used in sending other communications. There is no *invitation* or 'formal request' to a peer to join the list in Turnbull.

In addition, Turnbull and Aoki do not teach or suggest a *connect message* from the peer to a second member different from the first member, the connect message containing the first group membership certificate. Similar to that discussed above with respect to claim 2, verification of a user modifying a shared list in Turnbull is not a connect message from a peer to join a peer-to-peer group. Moreover, as noted above with respect to claim 2, neither Turnbull nor Aoki teach or suggest a *peer-to-peer group* of a peer to peer network. Accordingly, the combination of Turnbull and Aoki does not teach or suggest the features of claim 8.

Accordingly, claim 8 patentably distinguishes over Turnbull and Aoki such that the rejection under § 103 should be withdrawn. Claims 9–12 depend from independent claim 8, and are patentable for at least the foregoing reasons.

Claim 9

Claim 9 recites, *inter alia*, the method of claim 8 wherein the step of forming by the first member comprises the step of forming a group membership certificate having a structure  $((P_{U1})K_G)K_{U2}$ . In the Final Office Action, the Examiner suggests that Turnbull may be interpreted such that "the originating user [1] (i.e., the issuer) should also be required to be authenticated by the invited user [2] via validating the originating user's signature (i.e., using the additional the [sic] issuer's signature which is signed with  $K_{U2}$  in addition to  $((P_{U1})K_G)$ )" and cites Turnbull Col. 6, lines 20–23. (See, Office Action, page 4, 1st parag.).

Initially, Applicant assumes that the Examiner mistakenly switched the nomenclature of his suggested interpretation of Turnbull. Specifically, with respect to claim 2, the Examiner called the issuing user as user 1, and called the invited user as user 2. Applicant's assumption was not addressed in the Advisory Action, nor where

Type of Response: Amendment after FINAL

Application Number: 09/955,924

Attorney Docket Number: 177765.01

Filing Date: 09/19/2001

Applicant's arguments regarding claim 9 addressed. Applicant will continue with the nomenclature begun in the discussion of claim 2 and cited in the brackets within the Examiner's quotation above and restate the arguments traversing the rejection of claim 9.

The Examiner seems to suggest an interpretation of a combination of Turnbull and Aoki as having the issuer's signature *in addition* to the signature by the group private key). However, as noted above with respect to claim 2, the Examiner is already asserting that the group private key of Aoki *replaces* the issuing user's private key signature. Thus, Applicant is unable to determine how the same combination can teach the group key of Aoki as replacing *and* being in addition to the issuing user's private key. Moreover, this combination suggested by the Examiner is at odds with the Examiner's combination of the same references in the Advisory Action in rejecting claim 8 (e.g., the signed shared list of Turnbull is separate and independent of the signed certificate of Aoki). Even if Turnbull and Aoki in combination provided two independent certificates, these two independent certificates cannot then also teach signing the shared list of Turnbull with a key of the creating user in addition to a group key from Aoki.

Assuming without agreeing that the combination of Turnbull and Aoki teaches a group key signature in addition to the issuing user's signature, the combination does not teach signing the public key of a peer *first* with a group key and *then* with a group member's key. Specifically, there is nothing in Aoki and Turnbull which teaches or suggests the recited order of the signatures as recited in claim 9.

Accordingly, claim 9 patentably distinguishes over Turnbull and Aoki such that the rejection under § 103 should be withdrawn.

Claim 23

Claim 23 recites a computer-readable medium having computer executable instructions for performing the steps of claim 8. Accordingly, claim 23 is patentable for at least the foregoing reasons.

Rejection of claim 13-21, 24 and 25

Claims 13-15, 17, 18, 20, 21, 24 and 25 stand rejected under 35 U.S.C. § 103(a) as being obvious over Turnbull in view of U.S. Patent No. 6,266,420 to Langford et al. [hereinafter Langford]. Applicant respectfully traverses the rejection as follows:

Claim 13

Independent claim 13 recites, *inter alia*, receiving a group invitation from a first member containing an invitation certificate having a group ID provided therein and resolving the group ID to find a third member of the group different from the first member. The cited section of Turnbull in the Final Office Action, i.e., Col. 7 line 2-12, does not teach or suggest resolving the group ID to find a third member of the group. Specifically, the Examiner suggests in the Advisory Action that the 'invited' peer can resolve the shared list of Turnbull to determine a third member other than the first member. However, for the 'invited' peer to resolve the function group ID identified by the Examiner as the shared list, the 'invited' peer must have *access to the contents* of the shared list. To get such access, the 'invited' peer must be an *authorized user*, and not just an *invited* member. The Advisory Action does not clarify how an 'invited' user would resolve the shared list when it is not yet an authorized user of the list. Thus, Turnbull does not teach or suggest these features of claim 13.

Independent claim 13 also recites, *inter alia*, sending a connect message to the third member containing the invitation certificate signed with the private key. In this manner, claim 13 recites that the connect message to the *third member other than the*

Type of Response: Amendment after FINAL

Application Number: 09/955,924

Attorney Docket Number: 177765.01

Filing Date: 09/19/2001



*first member* includes the invitation certificate that is signed by a private key *of the peer*. The cited section of Turnbull in the Final Office Action (Col. 6 lines 20–23) does not teach or suggest these features of claim 13. Specifically, the cited section of Turnbull is a validation of the *originating user's* signature by a user accessing the list, and does not teach or suggest that the user accessing the list is the 'invited' user, nor that the accessing user *sends* this list to a third member identified in the list, nor that the list sent to the third member is *signed by the accessing user*. In this manner, claim 13 distinguishes over Turnbull, and thus, Applicant respectfully requests that the rejection under § 103 be withdrawn.

The Advisory Action does not address this feature of claim 13. However, in rejecting claim 18, the Advisory Action states that a connect message is a request message from the originator to invite the peer to validate the originator's signature. As noted above with respect to claim 2, Turnbull does not teach or suggest an invitation. Even if Turnbull taught such an invitation, Applicant is unable to determine how an invitation *from the originator* can be equated with connect message *from the peer*, much less a connect message to a *third member* other than the first member. Moreover, there is no teaching or suggestion in Turnbull that such a message would be signed by the *peer's own private key*. The shared list of Turnbull is signed with the private key of the originator. Thus, Turnbull does not teach or suggest the features of claim 13.

Independent claim 13 also recites, *inter alia*, receiving an accept message from the third member containing a group membership certificate signed by a private key of the third member. The Final Office Action cites Turnbull (i.e., col. 6 lines 20–23, and col. 7, lines 28–29) as suggesting an "ACCEPT" message from the user 2. However, Applicant is unable to find anywhere in the cited sections of Turnbull any reference to an accept message sent by a *third member* other than the first member, much less an

Type of Response: Amendment after FINAL

Application Number: 09/955,924

Attorney Docket Number: 177765.01

Filing Date: 09/19/2001

accept message which contains a group certificate, which is separate from the invitation certificate sent to the invited member by the first member as recited in claim 13. Since Turnbull does not teach or suggest the recited features of claim 13, Applicant respectfully requests that the rejection under § 103 be withdrawn.

This feature of claim 13 is not addressed in the Advisory Action. However, in the rejection of claim 18, the Advisory Action suggests that the accept message is the response message with respect to the request message as a result of signature verification. Applicant respectfully disagrees with the Examiner's characterization of Turnbull. As noted above, a user accessing the shared list may validate the list by verifying the originator's signature. However, the validation of the signature by the accessing user is not communicated to the originator in any way. Rather, the accessing user may contact the originator to receive the public key of the originator to validate the signature, but there is no teaching or suggestion in Turnbull that the *validation* of the signature is communicated to the originator. As such, there is no 'response message as a result of signature verification' as suggested by the Examiner. Accordingly, claim 13 distinguishes over the cited art, and Applicant respectfully requests withdrawal of the rejection of claim 13.

Applicant agrees with the Examiner statement in the Final Office Action that Turnbull does not teach or suggest receiving a group shared key to enable decryption of group traffic as recited in claim 13. However, the Examiner erroneously suggests that Langford, teaching a group communication process, may be combined with the shared list of Turnbull, since Langford specifically teaches away from such a combination. Specifically, the Examiner states in the Advisory Action regarding the rejection of claim 18 that the motivation to combine is "Turnbull teaches a shared list of multiple certificates that allows the end-user to obtain a certificate of other end-users without on [sic] a user-by-user basis ... and Langford further teaches an improving mechanism

Type of Response: Amendment after FINAL

Application Number: 09/955,924

Attorney Docket Number: 177765.01

Filing Date: 09/19/2001

to reduce the data overhead and therefore increase the system performance by providing an effective secure group communication that substantially reduces the data overhead accompanying each secure message in comparison using the security credentials of each of the member [sic].” However, Langford specifically rejects the communication method of Turnbull. More particularly, as noted above, the accessing user of Turnbull may use the individual public encryption keys in the certificates of the list to encrypt a message directly or to wrap a session key to communicate with those in the list. In contrast, Langford describes a directory list of a group of individual encryption keys in the Background section at Col. 1, lines 54–67. Langford continues to describe its own communication method as basing the security credentials on the group alone, and not of each member like Turnbull. (See, Langford, Col. 2, lines 36–44). Thus, Langford teaches away from using a shared list of Turnbull, and thus, should not be combined with Turnbull.

Since Turnbull in view of Langford does not teach or suggest all of the features of claim 13, claim 13 patentably distinguishes over Turnbull in view of Langford such that the rejection under § 103 should be withdrawn. Claims 14–17 depend from independent claim 13, and are patentable for at least the foregoing reasons.

Claim 24

Claim 24 recites a computer-readable medium having computer executable instructions for performing the steps of claim 13. Accordingly, claim 24 is patentable for at least the foregoing reasons.

Claim 18

Independent claim 18 recites, *inter alia*, receiving at a first member of the peer-to-peer group, a connect message from the peer containing an invitation certificate generated by a second member of the peer-to-peer group and signed by a private key of the peer. The cited sections of Turnbull do not teach or suggest receiving a connect

Type of Response: Amendment after FINAL

Application Number: 09/955,924

Attorney Docket Number: 177765.01

Filing Date: 09/19/2001

message from an 'invited' peer, the connect message containing an invitation certificate generated by a second member of the peer-to-peer group and signed by the private key of the invited peer. Rather, as noted above with respect to claim 2, the shared list of Turnbull is not an invitation certificate. Moreover, the 'invited' member does not send the shared list, even were it an invitation certificate. Rather, an authorized member of the group can only access the shared list. Moreover, as noted above with respect to claim 13, even if the 'invitation' were a connect message, such a connect message does not contain the shared list *signed* by the *invited peer*. Thus, Turnbull does not teach or suggest these features of claim 18.

Independent claim 18 also recites, *inter alia*, sending an accept message to the peer. The Examiner cites section of Turnbull, i.e., col. 6 lines 20–23, and col. 7, lines 28–29) as suggesting an "ACCEPT" message from the user 2. However, as noted above with respect to claim 13, Turnbull does not teach or suggest an accept message sent by a *first member* other than the second member. Since Turnbull does not teach or suggest the recited features of claim 18, Applicant respectfully requests that the rejection under § 103 be withdrawn.

Applicant agrees with the Examiner that Turnbull does not teach or suggest sending a group shared key to the peer as recited in claim 18. However, the Examiner erroneously suggests that Langford, teaching a group communication process, may be combined with the shared list of Turnbull. Specifically, as noted above with respect to claim 13, Langford specifically teaches away from such a combination, since it specifically rejects the communication method of Turnbull. Thus, Langford teaches away from using a shared list of Turnbull, and thus, should not be combined with Turnbull.

Since Turnbull in view of Langford does not teach or suggest all of the features of claim 18, claim 18 patentably distinguishes over Turnbull in view of Langford such

Type of Response: Amendment after FINAL

Application Number: 09/955,924

Attorney Docket Number: 177765.01

Filing Date: 09/19/2001

that the rejection under § 103 should be withdrawn. Claims 19–21 depend from independent claim 18, and are patentable for at least the foregoing reasons.

Claim 25

Claim 25 recites a computer-readable medium having computer executable instructions for performing the steps of claim 18. Accordingly, claim 25 is patentable for at least the foregoing reasons.

CONCLUSION

Accordingly, in view of the above amendment and remarks it is submitted that the claims are patentably distinct over the prior art and that all the rejections to the claims have been overcome. Reconsideration and reexamination of the above Application is requested. Based on the foregoing, Applicants respectfully requests that the pending claims be allowed, and that a timely Notice of Allowance be issued in this case. If the Examiner believes, after this amendment, that the application is not in condition for allowance, the Examiner is requested to call the Applicant's attorney at the telephone number listed below.

Type of Response: Amendment after FINAL  
Application Number: 09/955,924  
Attorney Docket Number: 177765.01  
Filing Date: 09/19/2001

**Reply under 37 CFR 1.116**  
**Expedited Procedure – Technology Center 2100**

If this response is not considered timely filed and if a request for an extension of time is otherwise absent, Applicants hereby request any necessary extension of time. If there is a fee occasioned by this response, including an extension fee that is not covered by an enclosed check please charge any deficiency to Deposit Account No. 50-0463.

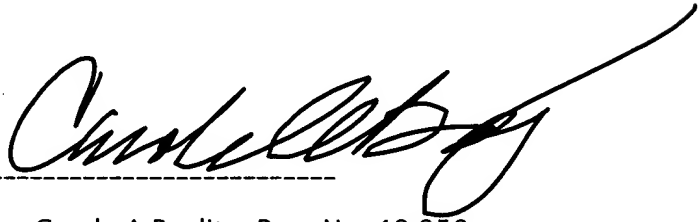
Respectfully submitted,

Microsoft Corporation

Date: \_\_\_\_\_

*11/10/05*

By: \_\_\_\_\_



Carole A Boelitz, Reg. No. 48,958  
Attorney for Applicants  
Direct telephone (425) 722-6035  
Microsoft Corporation  
One Microsoft Way  
Redmond WA 98052-6399

**EXPRESS MAIL CERTIFICATION UNDER 37 C.F.R. § 1.10**

Express Mail Mailing Label No.: EV 671529693 US

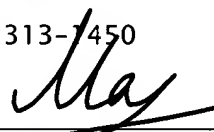
I hereby certify that this correspondence is being deposited with the United States Postal Service (USPS) as correspondence to be delivered by the "Express Mail Post Office to Addressee" service of the USPS on the date indicated below with sufficient postage in an envelope bearing the above-noted Express Mail mailing label number and addressed to:

Mail Stop RCE  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

November 10, 2005

Date

Signature \_\_\_\_\_



Kate Marochkina

Printed Name

Type of Response: Amendment after FINAL

Application Number: 09/955,924

Attorney Docket Number: 177765.01

Filing Date: 09/19/2001